Scytale AI, on behalf of Nebius B.V.
Schiphol Boulevard 165,
1118 BG Schiphol,
The Netherlands

Date: 25 August 2025

Confirmation of Compliance with the Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) is a regulatory framework of the European Union that came into effect on 17 January 2025 and applies to organizations within the financial services sector to ensure their digital operational resilience. This regulation mandates entities to implement robust measures to safeguard against ICT-related risks and ensure operational continuity under adverse circumstances.

As a responsible, forward-looking organization, Nebius B.V. acknowledges the significance of complying with DORA and has implemented appropriate measures at senior levels to enhance operational resilience and ICT risk management. Nebius B.V. is committed to meeting these regulatory obligations, ensuring preparedness against potential disruptions, and protecting stakeholders' interests effectively.

In alignment with DORA's requirements, Nebius B.V. has taken the following steps to achieve compliance:

1. A comprehensive policy for ICT risk management has been approved by senior management and effectively communicated across the organization.

2. Nebius B.V. has conducted a thorough identification and assessment of ICT-related risks and has implemented corresponding mitigation measures.
3. All employees have received training and awareness sessions on DORA's requirements and their individual responsibilities in maintaining operational resilience.
4. An incident management framework has been established to ensure the prompt detection, reporting, and resolution of ICT-related incidents, in compliance with DORA's requirements.
5. The organization has conducted business impact analyses and testing exercises to assess and validate the robustness of operational resilience measures.
6. Nebius B.V. has implemented a comprehensive ICT third-party risk management program to assess, monitor, and mitigate risks associated with outsourced service providers.
7. Procedures for reporting major ICT-related incidents to relevant regulatory authorities have been tested and verified.
8. Data integrity, confidentiality, and availability measures are in place to safeguard sensitive information in line with DORA's requirements.
9. Regular reviews and updates to ICT security policies, procedures, and controls are conducted to reflect evolving threats and regulatory expectations.
10. Contingency and recovery plans have been established, tested, and refined to ensure operational continuity in the event of ICT disruptions.

Nebius B.V., supported and assessed by Scytale AI, is committed to continuously improving ICT risk management and operational resilience in alignment with DORA and industry's best practices. This commitment ensures ongoing compliance with the regulation and upholds the trust and confidence of our stakeholders.

Should you have any questions or require further information regarding Nebius B.V.'s DORA compliance measures, please do not hesitate to contact us.

Sincerely,

Guy Horowitz
Chief Operations Officer
guy@scytale.ai